FEDERATION OF AMERICAN SCIENTISTS

T: 202/546-3300 1725 DeSales Street NW, 6th Floor, Washington, DC 20036 www.fas.org
F: 202/675-1010 fas@fas.org

September 10, 2013

Review Group on Intelligence and Communications Technologies

Dear Review Group Members:

I would like to offer the following comments and reflections on the issues facing the Review Group.

Introduction

The Presidential Memorandum of August 12, 2013 that established the Review group directed:

"The Review Group will assess whether, in light of advancements in communications technologies, the United States employs its technical collection capabilities in a manner that optimally protects our national security and advances our foreign policy while appropriately accounting for other policy considerations, such as the risk of unauthorized disclosure and our need to maintain the public trust."

Unfortunately, this Presidential instruction does not provide a crisp statement of the problem to be addressed. Instead, it invites the Review Group to ruminate on several undefined and incommensurate topics that could reasonably be interpreted or emphasized in multiple, divergent ways.

So in the following comments, I would like to propose some more narrowly focused questions that might help the Review Group to gain traction on this cluster of policy issues.

Is Current Practice Consistent with a Common Sense Reading of the Law?

One major source of public controversy is the perception that current intelligence collection policy, and specifically the practice of bulk collection of telephone

metadata, is inconsistent with a common sense reading of the law, which requires collection of US person data to be "relevant" to an authorized investigation.

The question here is not whether bulk collection is technically "illegal" but whether it is at odds with public assumptions and expectations. The fact that congressional leaders such as Rep. Sensenbrenner, an author of the USA PATRIOT Act, dispute the legitimacy of bulk collection is an indication of the force of this question.

If the Review Group believes that bulk collection of metadata is perfectly acceptable, then its deliberations can be swiftly concluded. But if it finds that bulk collection of US person data is not well-rooted in public statutes, then it will need to inquire further as to how this came about, and what to do about it.

What is the Nature and Magnitude of the Threat? Can Collection Practices be Modulated Accordingly?

A well-conceived intelligence apparatus would not be static but could be adjusted to adapt to evolving threats. The intensity and intrusiveness of intelligence collection should also vary in response to the magnitude of the threat.

In the event of a massive and overwhelming threat (e.g. the theft of an armed nuclear warhead) it would be appropriate to collect far more aggressively than under more non-emergency conditions, when such intrusive collection would be completely inappropriate and unacceptable.

Can the Review Group help to define a threat-based "escalation ladder" for intelligence collection that would start from a baseline of minimal intrusiveness that would only increase when there are credible indications of an increased threat?

Relatedly, <u>are there ways to help ensure that the adoption of intrusive intelligence measures can not only be modulated but also easily reversed or abandoned</u>?

I think one persistent source of public anxiety in this context is the concern that such intelligence measures, once adopted, will never be relinquished and will become a permanent part of American government. Is there a way to leave a trail of policy "bread crumbs" that would lead back to their eventual elimination?

Reduce Unauthorized Disclosures by Increasing the Integrity of Classification Decisions

I think it would be an error to view unauthorized disclosures of classified information primarily as a narrow problem of security policy that could be solved, perhaps, by a cleverly formulated new question on polygraph examinations.

Rather, as Senator Moynihan used to say, "If you want your secrets respected, make sure they are respectable." In other words, the best way to combat unauthorized disclosures is to prevent (or correct) the improper exercise of classification authority.

It is significant that both of the most prolific leakers of classified information in recent years, Pvt. Manning and Edward Snowden, have cast their disclosures as acts of conscience. They were rebelling against what they viewed as unjustified government secrecy. While this assertion does not inoculate them from criticism or liability, it would be a mistake to ignore it – particularly since the claim seems very well-founded in many respects. (The President himself has acknowledged "the problem of over-classification.")

Today, the Intelligence Community is responding to the Snowden disclosures with some accelerated declassification activity. This is welcome and commendable. But it would have been even more welcome a year ago or longer, when it might conceivably have averted the uncontrolled disclosures of recent months.

Therefore, I think the Review Group should propose a new policy process for adjudicating classification disputes.

Such a process would allow members of the public to "nominate" for expedited declassification review an issue area that is of current public interest but whose full dimensions are obscured by classification. The legitimacy of the current classification would then be submitted to review and evaluation by a panel of officials from outside of the originating agency. (So, for example, whether to acknowledge the role of CIA in targeted killing operations would no longer be up to CIA alone to decide, but would be determined by an interagency panel charged by the President with maximizing public disclosure.)

(An approach of this kind has proved remarkably effective in the case of the Interagency Security Classification Appeals Panel established by executive order 12958, which has overturned agency classification judgments in the majority of cases that it has reviewed. I wrote about this at greater length in a recent paper on "The Dynamics of Government Secrecy," Harvard Civil Rights-Civil Liberties Law Review, Summer 2013, available here: http://www.fas.org/sgp/eprint/dynamics.pdf .)

I think that efforts to focus new attention on the integrity of classification decisions would serve both to reduce unauthorized disclosures and to enhance public trust, another of the Review Group's objectives.

What Do We Want to Protect?

The Presidential Memorandum that established the Review Group seeks a policy that "optimally protects our national security and advances our foreign policy…."

This is a somewhat opaque formulation that obscures issues of concern to many people, particularly since the terms used are not defined.

I would say that what we want to optimally protect is not "national security" but "constitutional government." They are not exactly the same thing. In fact, the requirements of constitutional government often complicate or impede the pursuit of national security. So the distinction is an important one. The brute fact is that an insistence on constitutional government will sometimes entail risks that might otherwise be avoidable. And yet, as Americans, we do insist on it.

I think the Review Group could do a service by reminding readers of this admittedly elementary point.

Thank you for your consideration of these remarks. If they raise questions or if you would like any further elaboration, I would be pleased to respond.

With best wishes for your work,

Steven Aftergood
Federation of American Scientists
(202)454-4691
saftergood@fas.org